



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/031,065	04/02/2002	Jean-Sebastien Coron	032326-193	6065
21839	7590	11/08/2005	EXAMINER	
BUCHANAN INGERSOLL PC (INCLUDING BURNS, DOANE, SWECKER & MATHIS) POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404			POWERS, WILLIAM S	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 11/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center"><b>Office Action Summary</b></p>	<p><b>Application No.</b></p> <p>10/031,065</p>	<p><b>Applicant(s)</b></p> <p>CORON ET AL.</p>	
	<p><b>Examiner</b></p> <p>William S. Powers</p>	<p><b>Art Unit</b></p> <p>2134</p>	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 15 January 2002.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☒ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| <p>1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)</p> <p>2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)</p> <p>3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br/> Paper No(s)/Mail Date <u>1/15/2002</u>.</p> | <p>4) <input type="checkbox"/> Interview Summary (PTO-413)<br/> Paper No(s)/Mail Date. _____.</p> <p>5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)</p> <p>6) <input type="checkbox"/> Other: _____.</p> |
|---|---|

## **DETAILED ACTION**

### ***Claim Objections***

1. Claims 4-8 and 10-14 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The recitation "electronic device" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. Therefore, these claims stand or fall with their parent claims.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Art Unit: 2134

1. Claims 1-3 and 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the integer variable  $y$ " in page 3, line 5 of the preliminary amendments. There is insufficient antecedent basis for this limitation in the claim.

Claim 2 recites the limitations "[r]eplace  $s$  with  $s$ " in page 3, line 20 of the preliminary amendments and "[p]ut in  $x_i$ " in page 4, line 3 of the preliminary amendments. There are insufficient antecedent bases for these limitations in the claim.

Claim 2 recites the phrase "quality deemed to be insufficient of random integers on 64 bits" (page 3, lines 15-16 of the preliminary amendments) which is indefinite language. It is not clear from the claim language how one of ordinary skill in the art would determine whether integers are of sufficient quality to satisfy the limitations of the claim.

Claim 3 recites the limitation " $x_m$ " in page 4, line 20 of the preliminary amendments. There is insufficient antecedent basis for this limitation in the claim.

Claim 9 recites the limitation " $x_i$ " in page 6, line 3 of the preliminary amendments. There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 1 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim manipulates abstract data and output said manipulated abstract data, which is not tangible.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-14 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,028,939 to Yin.

Art Unit: 2134

As to claims 1-3 and 9, Yin teaches the use of the DES algorithm in generating random numbers in an iterative manner using the Boolean operator exclusive OR (column 5, lines 12-53 and figure 2B).

As to claims 4-8 and 10-14, the modifications to the preamble stand or fall with the claims that recite the preamble. As a result, the limitations are assumed to be covered by the art that reads on the independent claims.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 4, 5, 6, 7, 10, 11, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,028,939 to Yin in view of U.S. Patent No. 6,278,783 to Kocher et al. (hereafter referred to as Kocher).

As to claim 4, 5, 6, 7, 10, 11, 12 and 13 Yin teaches a data security system that embodies a DES chip or a custom ASIC device to perform DES algorithms (column 4, lines 1-26), but does not expressly mention the device being a smart card, contactless card, ID badge or PCMCIA card.

Art Unit: 2134

Kocher teaches a data security system that uses the DES algorithm that can be embodied in several different form factors including smart cards, contactless cards, electronic badges and PCMCIA cards (column 14, lines 1-39) in order to "construct devices that are significantly more resistant to attack" (column 13, lines 61-62).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Yin with the devices mentioned by Kocher in order to "construct devices that are significantly more resistant to attack" (Kocher, column 13, lines 61-62).

5. Claims 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,028,939 to Yin in view of U.S. Patent Application No. 2004/0040026 to Farrugia.

As to claims 8 and 14, Yin teaches a data security system that embodies a DES chip or a custom ASIC device to perform DES algorithms (column 4, lines 1-26), but does not expressly mention the device being a smart watch.

Farrugia teaches the use of a smart device such as a smart watch that has the capability to execute programs and applications (paragraph 24) in order to "provide enhanced flexibility and interoperability among different smart device types" (paragraph 63, lines 7-8).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Yin with the smart watch mentioned

Art Unit: 2134

by Farrugia in order to "provide enhanced flexibility and interoperability among different smart device types" (paragraph 63, lines 7-8).

### ***Conclusion***

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,327,661 to Kocher et al. discloses the use of smart cards in cryptosystems.

U.S. Patent No. 5,793,871 to Jackson discloses the use of the DES algorithm.

U.S. Patent No. 6,044,388 to DeBellis et al. discloses a random number generator, the DES algorithm and applying the exclusive OR operation to the random numbers in intermediate steps.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers, whose telephone number is (571) 272-8573. The examiner can normally be reached Monday-Thursday from 8 AM – 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

**Any response to this action should be mailed to:**



Art Unit: 2134

Commissioner of Patents and Trademarks  
PO Box 1450  
Alexandria, VA 22313-1450

**Or faxed to:**


(571) 273-8300

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (886) 217-9197 (toll-free).

  
WSP

October 24, 2005

  
COPY TO BE  
SENT TO THE  
PATENT OFFICE